## REMARKS

This application has been carefully reviewed in light of the Office Action dated May 4, 2005. Claims 1 to 5 and 7 to 34 are in the application, of which Claims 1, 22, 23, 27, 28, 31 and 34 are all independent. Reconsideration and further examination are respectfully requested.

Two replacement drawing sheets are submitted herewith, for Figures 3 and 7. These replacement drawing sheets address the objections lodged by the Office Action against the drawings, namely the objection at paragraph 1 for duplicate reference numerals in Figure 3, and at paragraph 3 for an incorrect labeling of decryption algorithm 92.

The specification has been amended so as to address the objection lodged against the drawings in paragraph 2 of the Office Action. In particular, descriptions for omitted reference numerals have been inserted at pages 17, 18 and 30 of the specification. In view of the foregoing changes to the specification and to the drawings, withdrawal of the drawing objections is respectfully requested.

A new abstract has been submitted, so as to comply with the PTO's guideline of a 150 word length.

Paragraph 5 of the Office Action entered an objection to the specification stating that while certain abbreviations were well-known in the art, they should be defined anyway. Applicants agree that these abbreviations are well-known in the art, such that a definition hardly seems necessary; nevertheless, the requested definitions have been inserted at pages 13 and 16.

Claim 27 was rejected under 35 U.S.C. § 112, second paragraph. In response, the "storage means" at line 13 thereof has been changed to "storing means". Withdrawal of the rejection is respectfully requested.

All claims were rejected under 35 U.S.C. § 103(a) primarily over U.S. Patent 6,711,677 (Wiegley), or over Wiegley in view of U.S. Patent 5,953,419 (Lohstroh), U.S. Patent 6,470,450 (Langford), or U.S. Patent 6,473,508 (Young). All rejections are respectfully traversed.

The invention concerns secure storage of a public key for encryption of data in a computing device that includes a user-specific key pair which is securely stored in the computing device. A target public key is received corresponding to a target device, and a user-specific key pair is obtained from a secure registry. The user-specific key pair includes a user-specific private key and a user-specific public key. The user-specific private key is utilized to create a target key verifier based on the target public key. The target key verifier is stored together with a target public key in a storage area. Thereafter, the target key verifier and the target public key are retrieved from the storage area, and a user-specific public key is applied to the target key verifier for verifying authenticity of the target public key. Data is encrypted when the target public key of authenticity of the target public key is verified, thereby creating encrypted data for transmission to the target device.

Accordingly, it is a feature of the invention that authenticity of a target public key is verified, such as by application of a user-specific public key from a user-specific key pair to a target key verifier. One purpose of such a verification is to verify whether or not the public key has been corrupted or modified by an unauthorized intruder,

in order to confirm that the public key is safe to use. If authenticity of the target public key is verified, the data is encrypted thereby creating encrypted data for transmission to a target device.

In entering the rejection of the claims, the Office Action acknowledges that Wiegley does not disclose encryption of data with a target public key, but rather shows encryption of data with a session key. Moreover, the Office Action acknowledges that Wiegley does not disclose that encryption of data with the target public key is conditioned on verification of the authenticity of the target public key. According to the reasoning in the Office Action, however, these differences are not sufficient to differentiate the invention from Wiegley or Wiegley in the combinations proposed in the Office Action.

It is respectfully submitted that unwarranted conclusions have been drawn from Wiegley, based on broad speculation and inferences not supported by art-based evidence. Moreover, it is respectfully submitted that no rationale has been articulated as to why those of ordinary skill would have been motivated to change the disclosure of Wiegley as proposed in the Office Action. This is explained more fully below.

As understood from Wiegley, the session key in Wiegley is a private key used to encrypt print data when sending the print data from a printer client to a printer. In the embodiment described by Wiegley, the session key is encrypted with a public key to avoid wire tapping, and the encrypted session key is thereafter sent from the printer client to the printer. As recognized in the Office Action, this disclosure is not the same as verification according to the invention, and it is also not the same as data encryption according to the invention.

Wiegley also describes a session identification (hereinafter "session ID"). The session ID is information which is issued by a printer to be stored in a printer client and sent back to the printer from the printer client. The session ID is also information to identify the printer client and is sent to the printer from the printer client accompanied with the print data. The session ID is verified at the printer, and if it has not changed from a previously-received session ID, the printer prints the print job.

Thus, in Wiegley, the purpose of verifying the session ID (i.e., to determine whether or not it ha been modified from a previously-received session ID) is to confirm that the print job is sent from the same printer client which accessed it previously. On the other hand, verification according to the invention is to verify whether or not the public key has been modified in order to confirm that the public key is safe to use. Accordingly, the disclosure of Wiegley is fully different in their purposes and structures from the invention, particularly as regards verification and data encryption according to the invention.

The remaining art applied against the claims, namely Lohstroh, Langford and Young, has all been reviewed, but it is not seen to remedy any of the above-noted deficiencies of Wiegley. It is noted, in particular, that the Office Action does not rely on those patents for any of the above-noted features, but rather relies on Wiegley for reasons that are incorrect, as explained above.

It is therefore respectfully submitted that the claims herein define subject matter that would not have been obvious from Wiegley or Wiegley in combination with the cited secondary references. Allowance of the claims is respectfully requested.

Applicants' undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicants
Michael K. O'Neill
Registration No. 32,622

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3800
Facsimile: (212) 218-2200

CA_MAIN 102948v1